Sistema
BIOMÉTRICO inteligente
mod. MF830
(Control de ACCESO y PRESENCIA por huella dactilar)

ÍNDICE

1.	**ELEMENTOS QUE INTEGRAN EL SISTEMA**	**4.-**
2.	**BREVE DESCRIPCIÓN DEL FUNCIONAMIENTO DEL SISTEMA**	**5.-**
3.	**ESTRUCTURA DEL MENÚ**	**8.-**
4.	**FUNCIONES MENÚ GESTIÓN DE DATOS (Dar de alta)**	**13.-**
4.1.	Registro de altas de ADMINISTRADOR	13.-
4.2.	Registro de altas de USUARIOS	16.-
4.3.	Nivel de configuración	17.-
4.4.	Función BORRAR	18.-
4.5.	Borrar todos los LOG	19.-
5.	**MENÚ CONFIGURACIÓN**	**19.-**
5.1.	Sistema	19.-
5.2.	Configuración bloqueo (funciones CONTROL DE ACCESOS)	20.-
5.3.	Comunicación	25.-
5.4.	Configuración LOG	28.-
6.	**MENÚ INFORMACIÓN DEL SISTEMA**	**29.-**
7.	**ESPECIFICACIONES Y ESQUEMAS TÉCNICOS**	**30.-**
7.1.	Especificaciones técnicas	30.-
7.2.	Esquemas técnicos	31.-

Gracias por adquirir nuestro sistema de control de presencia por huella digital.

Para el correcto uso y funcionamiento del mismo, es importante lea detenidamente el presente manual de instrucciones.

1. ELEMENTOS QUE INTEGRAN EL SISTEMA

El sistema biométrico mod. MF830 se suministra con los siguientes elementos:

-Terminal

-Interface de comunicación

-Cable 16 hilos para control accesos

-Chapa para instalación del terminal en paredes

-Manual de usuario del terminal

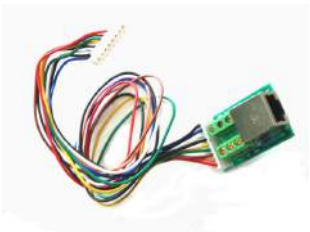
-Software de gestión

-Manual de usuario del software de gestión

Terminal MF830

Chapa fijación a pared

Software y manuales



Interface comunicación

Cable 16 hilos

2. BREVE DESCRIPCIÓN DEL FUNCIONAMIENTO DEL SISTEMA

► Ubicación del lector de huellas

El lector de huellas ha sido diseñado para poder ubicarse en posición sobremesa o fijado a la pared. Para esta última se suministra junto con el equipo una chapa metálica negra (debe fijarse a la pared), provista de unos ganchos sobre los cuales finalmente descansará el equipo.

A la hora de fijar la chapa se debe prever la no existencia de campos magnéticos o eléctricos próximos.

► Ambiente de operación

Para asegurar el rendimiento óptimo del equipo, éste deberá funcionar bajo un rango de temperaturas comprendido entre 0 y 60ºC

Por favor evite caídas y golpes bruscos del equipo. Esto afectaría seguro al funcionamiento normal del sistema.

► Breve descripción del sistema

El sistema de lector de huellas mod. MF830 está conformado por un TERMINAL y por una APLICACIÓN (software) encargada de gestionar la información recogida por aquel.

El TERMINAL es el principal responsable del registro de empleados mediante el uso de sus huellas dactilares, y recoge la información relativa a las diferentes entradas/ salidas que el personal de la empresa realiza. Este terminal permite también el registro de empleados mediante el uso de TARJETAS DE PROXIMIDAD (*) y CLAVE NUMÉRICA.

(*) Necesita la conexión de un lector de tarjetas (EM) externo, no incluido.

La APLICACIÓN (software) trata la información recogida por el terminal y permite la generación de diferentes informes, estadísticas y listados en base a filtros y criterios aplicados por el administrador responsabilizado por la empresa.

Si bien el terminal MF830 es autónomo (almacena y presenta la información sin necesidad de instalar el software), el tratamiento y la visualización de la información desde la aplicación es mucho más versátil y afable.

El terminal también está diseñado para registrar entradas y salidas de caracter especial (pausa para fumar, visita al médico, etc.) Los denominamos FICHAJES ESPECIALES y se activan y configuran desde la aplicación de software. La secuencia a teclear en el terminal para un fichaje especial tendría la siguiente estructura:

Tecla OK + código especial (1,2,3, etc.) + tecla OK + huella/ tarjeta de proxi./ clave

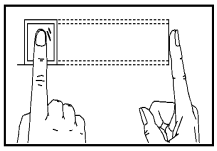
Existen 2 modos de comunicación entre el Terminal y el Ordenador que aloja el software: TCP/IP y RS485.

► **Método de lectura de huella**

Una vez realizada la configuración del terminal, según se describe en capítulos posteriores, el lector de huellas estará preparado para la recogida de información.

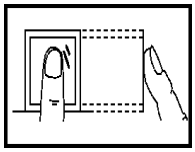
Para que se realice una lectura correcta de la huella, es importante ceñirse a las recomendaciones que se describen en los dibujos adjuntos.

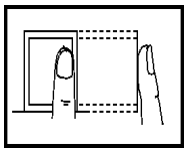
El dedo recomendado para el registro de huella es el dedo "índice", y debe posicionarse en la ventana de lectura tal y como se describe en la figura inferior.



correcto

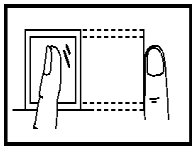
Muy perpendicular

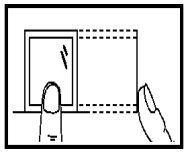




Poco centrado

Poco apoyo





Muy bajo

► Teclado

La disposición del teclado se ajusta a la descrita en el dibujo adjunto (figura 2-1):

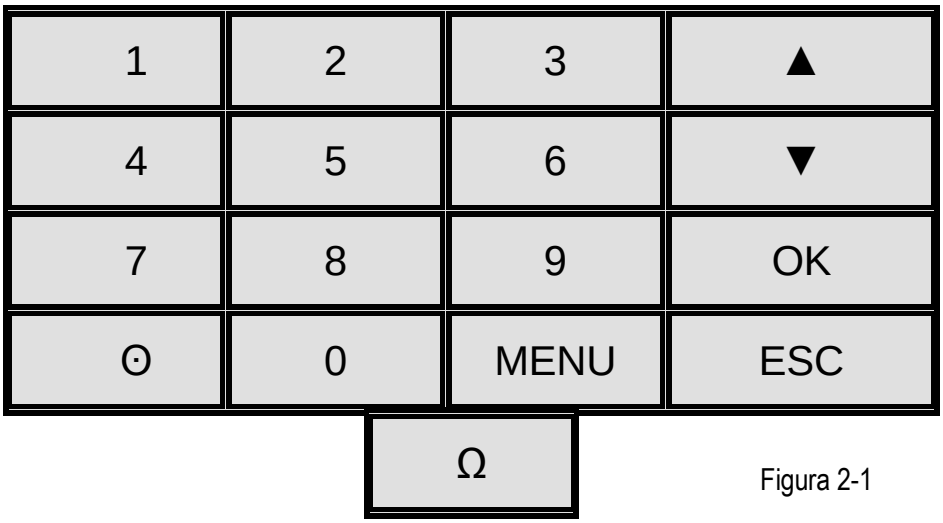


Figura 2-1

Las funciones de las diferentes teclas se describen en el cuadro inferior

***ESC:**	Para cancelar opciones dentro del menú y para desplazarse hacia atrás dentro de los diferentes niveles de éste
***MENU:**	Para acceder a los diferentes parámetros y funciones de configuración.
***OK:**	Para confirmar las diferentes opciones presentadas en el menú.
*⊙:	Para encender/ apagar el equipo.
*▲:	Para desplazarse hacia arriba por las diferentes opciones presentadas en el menú.
*▼:	Para desplazarse hacia abajo por las diferentes opciones presentadas en el menú
* 0...9:	Para introducir números según configuraciones solicitadas.
* Ω :	Timbre

3. LA ESTRUCTURA DEL MENÚ

El terminal se configura por medio del teclado del equipo y a través de una estructura de menús y submenús que contemplan todas las funciones y ajustes.

Nivel 1 (principal):

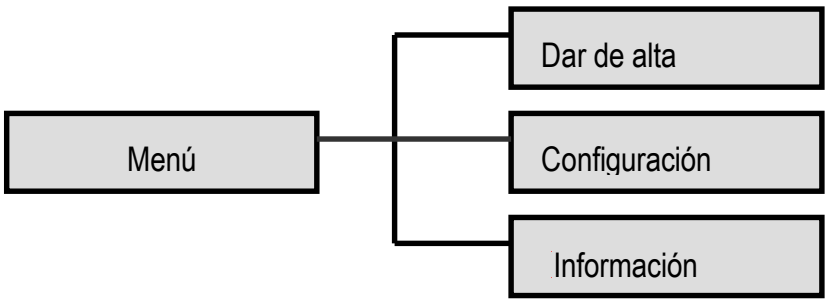
► **Gestión de datos (Dar de alta)**: para registrar y borrar huellas, claves o tarjetas, tanto en administradores como usuarios y configurar funciones como verificación y descarga de registros, niveles de seguridad, etc.

► **Configuración**: parametrización de aspectos tales como el sistema de comunicación a emplear, formato de presentación en pantalla, etc.:

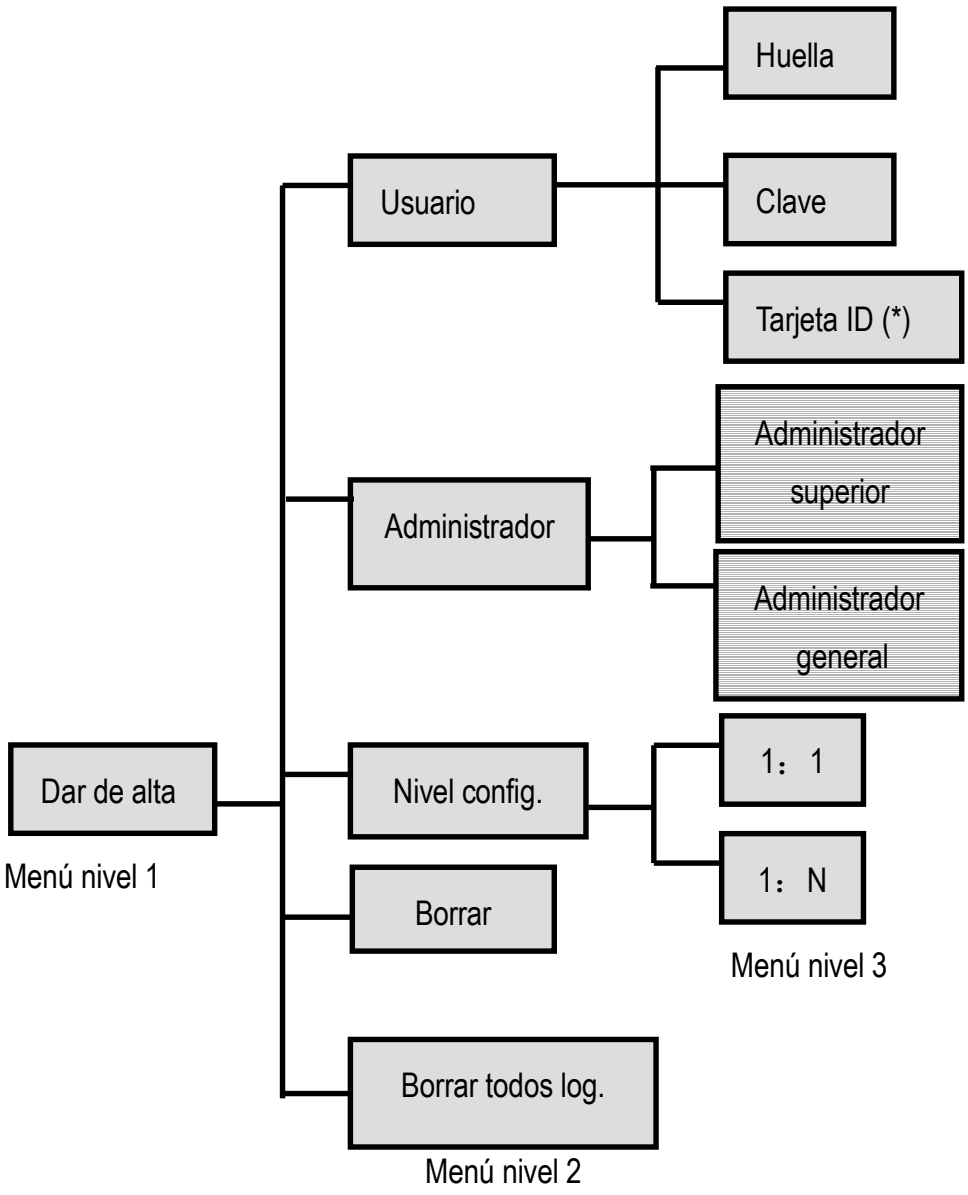
► **Información del sistema**: para examinar la información almacenada en el terminal.

El diagrama del menu principal (nivel 1) quedaría de la siguiente manera:

Menú PRINCIPAL

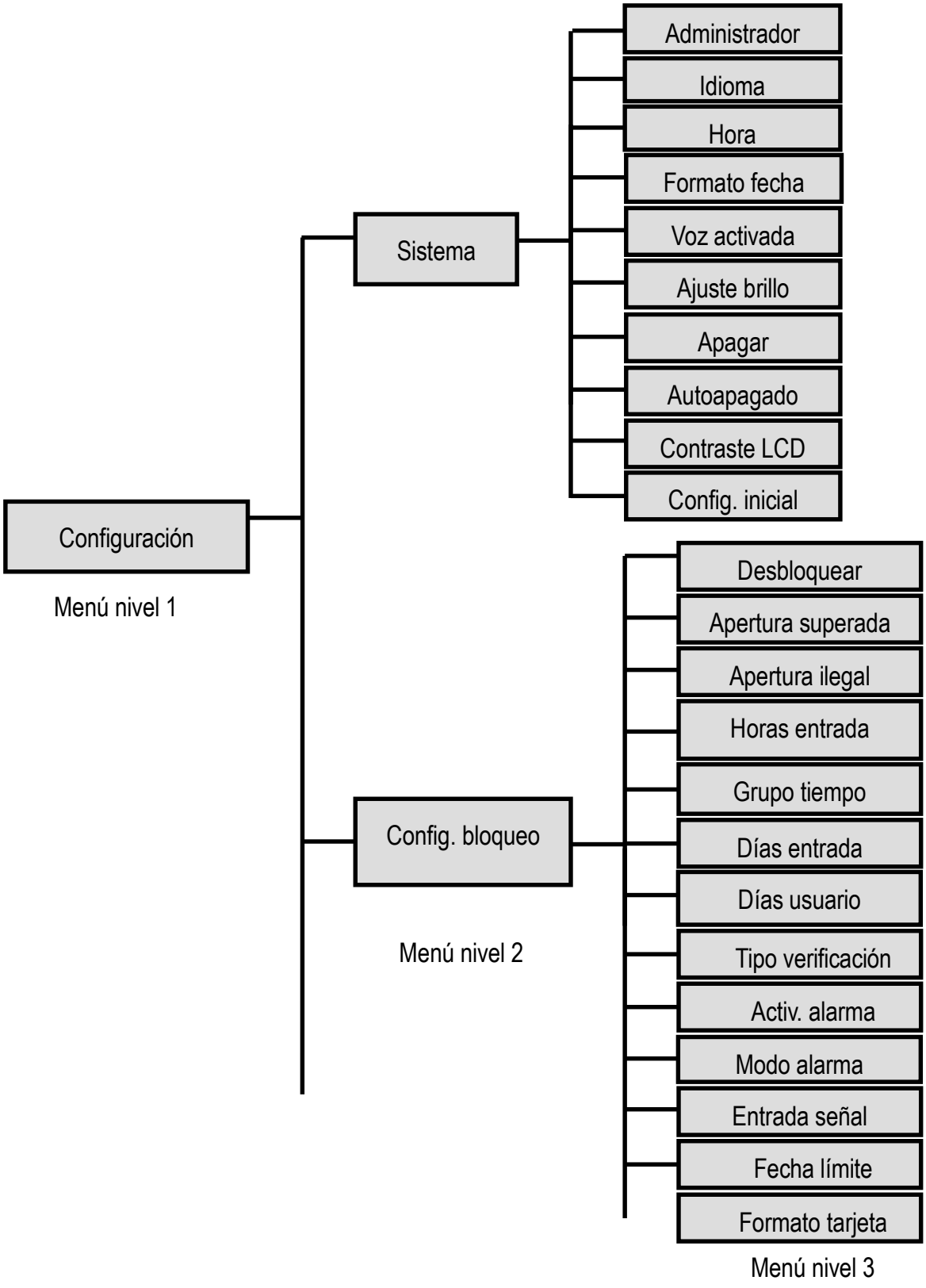


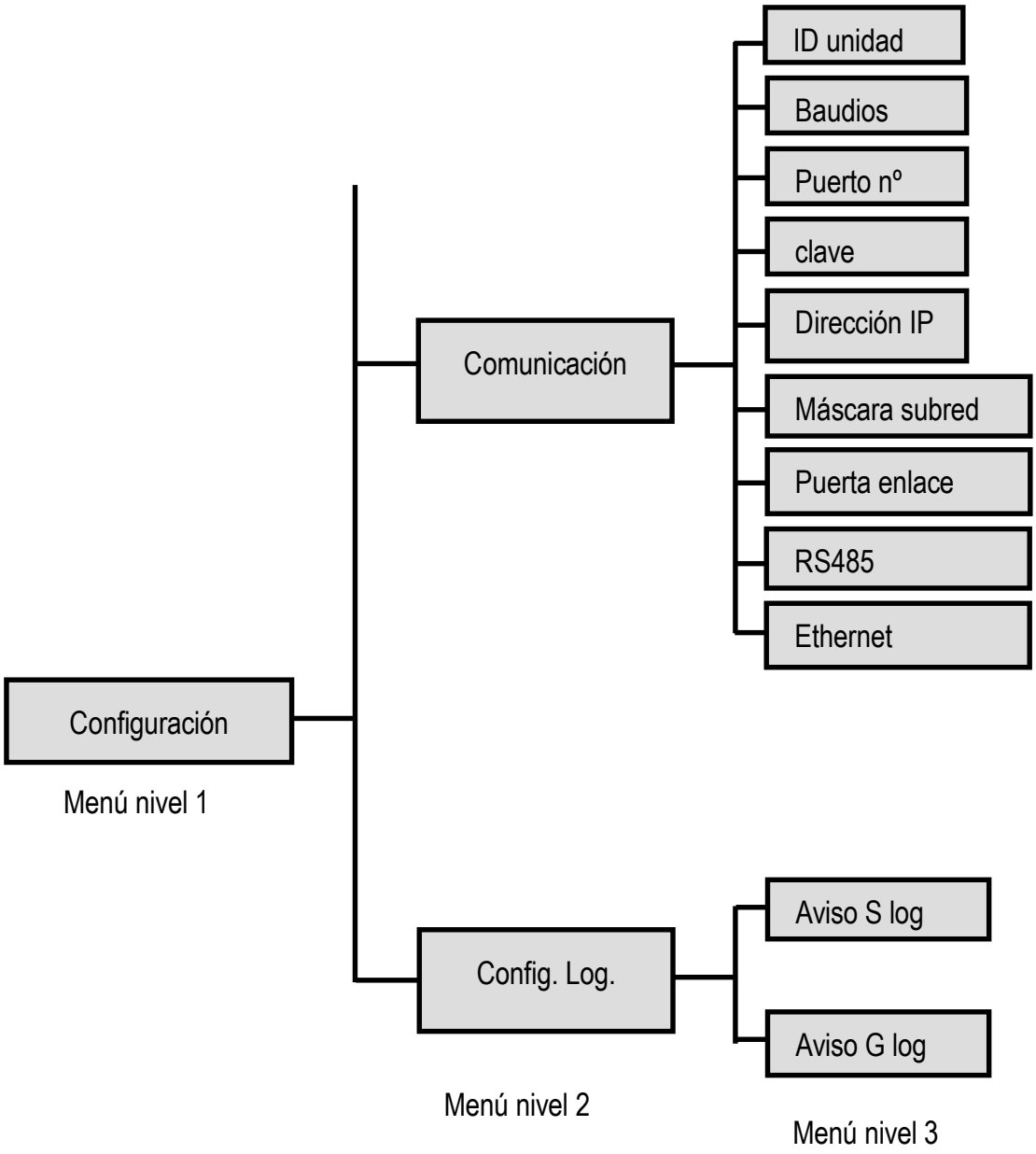
Menú GESTIÓN DE DATOS (dar de alta). Submenús.



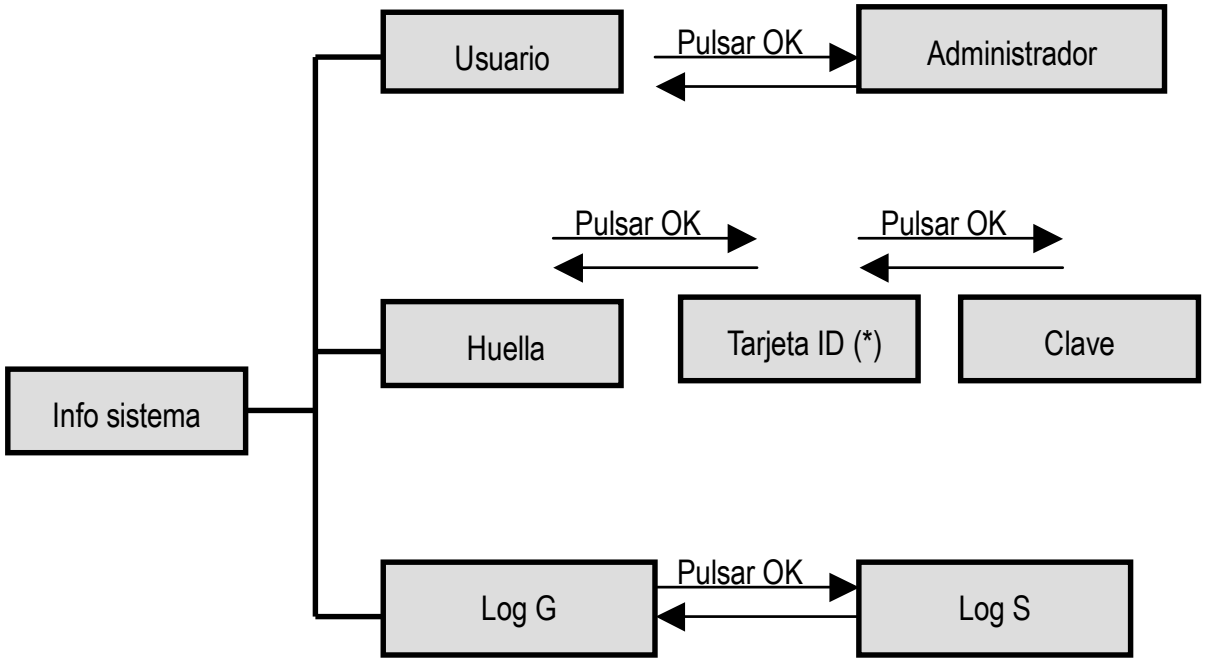
(*)Lector de tarjetas ID no incluido en el terminal. Para esta función se necesita la conexión previa de un lector de tarjetas ID externo.

Menú CONFIGURACIÓN. Submenús




ID unidad
Baudios
Puerto nº
clave
Dirección IP
Comunicación
Máscara subred
Puerta enlace
RS485
Ethernet
Configuración
Menú nivel 1
Aviso S log
Config. Log.
Aviso G log
Menú nivel 2
Menú nivel 3

Menú INFORMACIÓN DEL SISTEMA. Submenús



(*)Lector de tarjetas ID no incluido en el terminal. Para esta función se necesita la conexión previa de un lector de tarjetas ID externo.

Nota:

Desde las opciones del nivel de menú 2, y pulsando la tecla OK, conmutaremos a las otras opciones, según se representa en el dibujo superior.

(Ej.: Opción USUARIO + tecla OK = opción ADMINISTRADOR)

FUNCIONES DEL MENÚ

Una vez encendemos el equipo, accedemos a la pantalla de bienvenida, según se detalla en el dibujo adjunto.

Desde ella y presionando la tecla MENÚ, entramos en la pantalla de opciones principales, dentro de la cual se encuentra el menú DAR DE ALTA, que ahora trataremos.

4. FUNCIONES MENÚ GESTIÓN DE DATOS (Dar de alta)

4.1. Registro de ALTAS de ADMINISTRADOR

Si bien en el menú gestión de datos la primera opción es el registro de altas de USUARIO, detallaremos previamente el de ADMINISTRADOR ya que se entiende que serán estos únicamente los responsables de la gestión de altas de los usuarios. Si no se dieran de alta administradores, cualquier usuario podría gestionar el alta de otros usuarios y acceder a todas funciones y configuraciones del equipo. Se podrán dar de alta hasta un máximo de 10 administradores.

► **Administrador SUPERIOR**

El administrador SUPERIOR será el que tenga acceso a TODAS las funciones y configuraciones del equipo.

► **Administrador GENERAL**

El administrador GENERAL tendrá sólo acceso a determinadas funciones tales como “Alta

de usuarios", "Eliminación de registros de altas", etc.

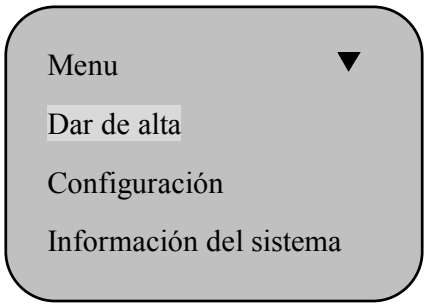
Tanto el administrador superior como el general, podrán registrarse en el sistema por medio de HUELLA DACTILAR, TARJETA DE PROXIMIDAD (*) y CONTRASEÑA.

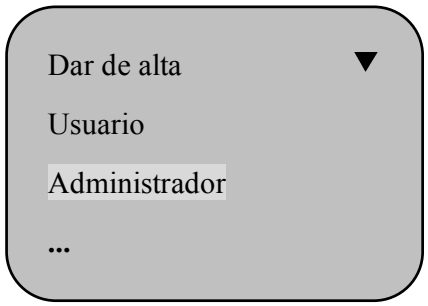
(*)Lector de tarjetas ID no incluido en el terminal. Para esta función se necesita la conexión previa de un lector de tarjetas ID externo.

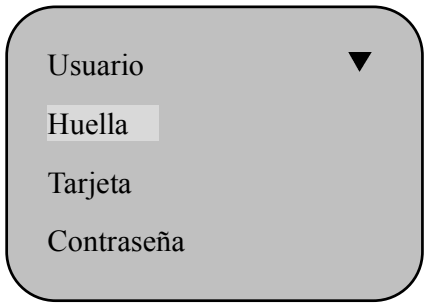
► Registro de altas de ADMINISTRADOR por HUELLA DACTILAR

Desde la pantalla de bienvenida pulse la siguiente secuencia de teclas:

MENÚ/ DAR DE ALTA/ ADMINISTRADOR/ SUPERIOR ó GENERAL/ HUELLA, recorriendo las pantallas tal y como se muestra en los dibujos inferiores.

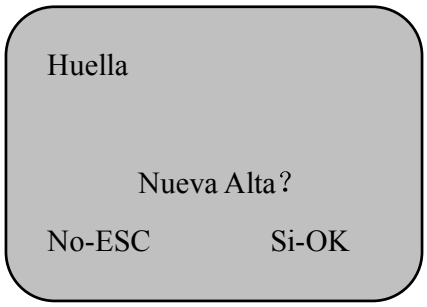


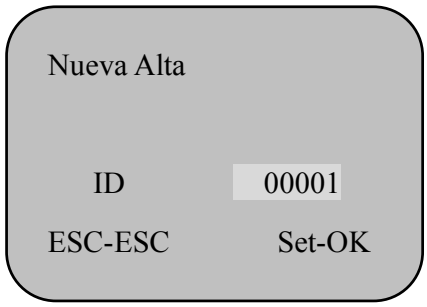


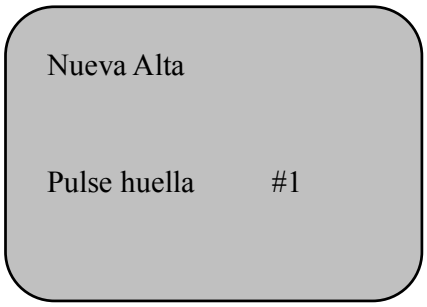


En la siguiente pantalla nos preguntará si se trata de un alta nueva (hay que tener en cuenta que cada administrador podrá registrar hasta 3 huellas diferentes, 1 tarjeta de proximidad y 1 contraseña). Por tanto si pulsamos OK accederemos al registro de un administrador nuevo, cuyo ID será el inmediatamente siguiente al último que se dió de alta. Por el contrario si pulsamos ESC, podremos luego introducir por medio del teclado numérico el ID de administrador sobre el que queramos realizar el nuevo alta de huella.

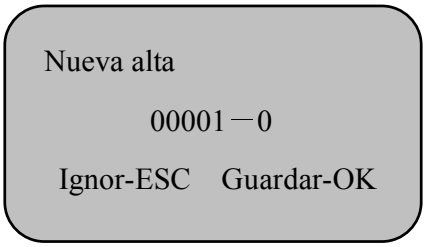
Para teclear el ID no es necesario pulsar los ceros precedentes (ej.: no 00005, sino 5 directamente). En ambos casos el sistema nos pedirá que pulsemos hasta 3 veces con el dedo en el lector situado dentro de la ventana de registro.







Después del tercer registro de la huella el sistema nos pedirá confirmación para así realizar la grabación del alta.

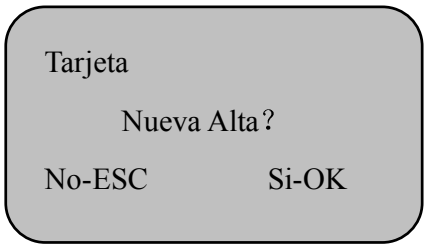


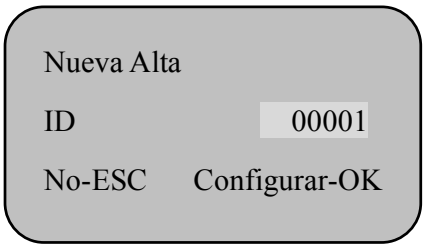
NOTA:

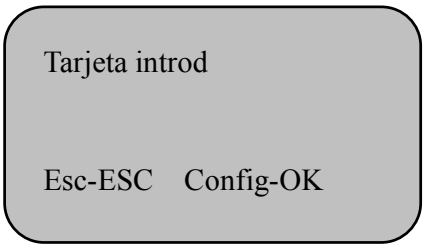
00001- 0 **el último dígito (0), indica la grabación de la primera huella

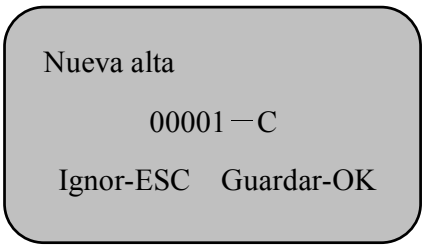
► Registro de altas de ADMINISTRADOR por TARJETA DE PROXIMIDAD (*)

El proceso es el mismo que el descrito en el registro por huella, teniendo en cuenta que en lugar de pedirnos que registremos nuestra huella, el sistema nos pedirá que registremos la tarjeta.









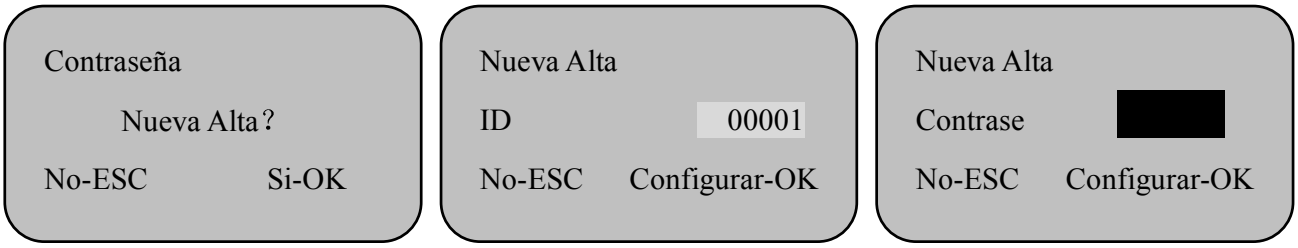
NOTA:

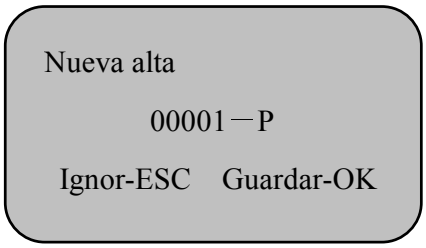
00001- C **La C indica que el registro es de tipo tarjeta (card)

(*)Lector de tarjetas ID no incluido en el terminal. Para esta función se necesita la conexión previa de un lector de tarjetas ID externo.

► Registro de altas de ADMINISTRADOR por CONTRASEÑA.

El proceso es el mismo que el descrito en el registro por huella, teniendo en cuenta que en lugar de pedirnos que registremos nuestra huella, el sistema nos pedirá que introduzcamos y confirmemos una clave numérica (máximo 4 dígitos).





NOTA:

00001- P **La P indica que el registro es de tipo contraseña (password).

4.2. Registro de ALTAS de USUARIO

El proceso es el mismo que el descrito en el registro de Administradores, teniendo en cuenta que si se han registrado previamente administradores, sólo estos podrán gestionar el alta de usuarios.

Los usuarios podrán podrán registrarse en el sistema por medio de HUELLA DACTILAR, TARJETA DE PROXIMIDAD(*) y CONTRASEÑA.

(*)Lector de tarjetas ID no incluido en el terminal. Para esta función se necesita la conexión previa de un lector de tarjetas ID externo.

El sistema admite un total de 2.000 altas entre usuarios y administradores.

► **Registro de altas de USUARIO por HUELLA DACTILAR**

El proceso es el mismo que el descrito en el registro de administradores por huella.

► **Registro de altas de USUARIO por TARJETA DE PROXIMIDAD**

El proceso es el mismo que el descrito en el registro de administradores por tarjeta.

► **Registro de altas de USUARIO por CONTRASEÑA.**

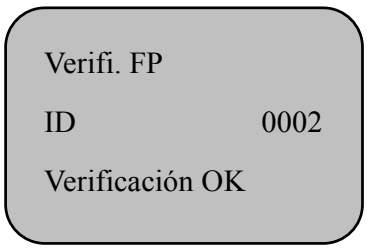
El proceso es el mismo que el registro de administradores por contraseña.

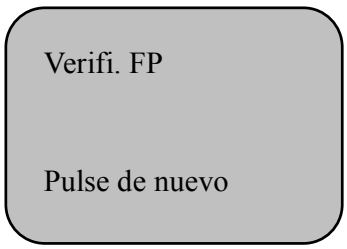
Una vez que se han dado de alta los registros, es interesante verificar que la lectura de los mismos se realiza de forma correcta. Para ello probaremos a introducir nuestra huella o contraseña y esperaremos confirmación del terminal.

-Con función voz activada (capítulo 5.1): si la lectura es correcta el sistema dirá **"identificación válida",** de lo contrario dirá: **"repita identificación"** y se mantendrá a la espera.

-Con función voz desactivada (capítulo 5.1): si la lectura es correcta el sistema presentará en pantalla **"Verificación OK",** de lo contrario presentará **"pulse de nuevo"** y se mantendrá a la espera.

En ambos casos el sistema también acompañará la confirmación o no de la lectura con pitidos diferentes





4.3. Nivel de CONFIGURACIÓN

Este apartado se refiere al establecimiento de los niveles de sensibilidad que primarán en el

momento de realizar la lectura de la huella. En general, el nivel de seguridad se equilibra entre los valores FAR (referido a que el terminal, de forma errónea, reconoce la huella del usuario A como si fuera la del usuario B) y FRR (referido a que el terminal, de forma errónea, rechaza la huella de un usuario registrado previamente de forma correcta).

La configuración se realiza en los 2 siguientes niveles:

► **Nivel 1:N: valores entre (1 – 4), valor por defecto (1)**

*Este es un nivel de sensibilidad que se aplica a TODOS los usuarios registrados.

► **Nivel 1:1: valores entre (0 – 50), valor por defecto (27)**

*Este es un nivel de sensibilidad que debe aplicarse sólo a aquellos usuarios ante los que el terminal pudiera presentar problemas para leer su huella (suciedad, huella dañada, etc.). En estos casos el valor debe reducirse para que el sistema sea "menos exigente" al realizar la lectura de la huella.

4.4. Función BORRAR

Desde la pantalla de bienvenida pulse la siguiente secuencia de teclas:

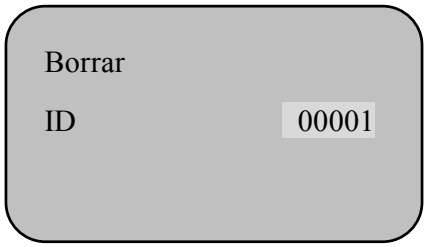
MENÚ (si hay activados administradores el sistema pedirá huella o clave para permitir acceso)/ DAR DE ALTA/ BORRAR, para eliminar registros de administradores y usuarios.

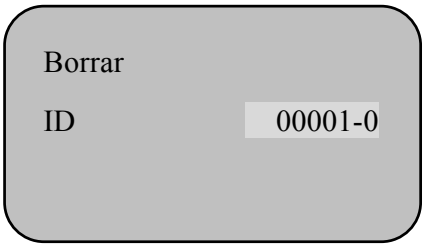
Según se detalla en las figuras de abajo, el sistema nos preguntará el ID del usuario / administrador que queremos borrar. Cuando confirmemos este punto, aparecerá una nueva pantalla en la que se nos preguntará el nº de huella (recordemos que pueden registrarse hasta 3 por cada usuario/ administrador), tarjeta (recordemos que puede registrarse solamente una por cada usuario/ administrador) y contraseña (solamente una por cada usuario/ administrador) que queremos eliminar. Si queremos borrar todas las huellas / tarjeta / contraseña de un usuario/ administrador, bastará con que confirmemos sucesivas veces con la tecla OK ya que el sistema nos irá presentando sucesivamente en pantalla los diferentes números de huella, tarjeta y contraseña activos con ese usuario/ administrador.

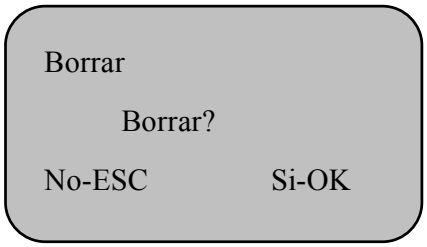
Si sólo queremos borrar un nº de huella determinado o sólo la tarjeta o sólo la contraseña, desde la pantalla que representa el dibujo 2, utilizaremos las teclas ▲▼ para movernos por

todos los registros activos de ese usuario/ administrador.

(En el dibujo 2 el dígito –0 indica la huella nº 1 registrada)







-Dibujo 2- -Dibujo 3-

Finalmente, el sistema nos pedirá confirmación para borrar el registro seleccionado. (dibujo 3).

4.5. BORRAR Todos los LOG

Permite borrar de golpe todos los datos relativos a las entradas y salidas realizadas por los diferentes usuarios/ administradores.

5. MENÚ CONFIGURACIÓN

Este menú nos dará acceso a los submenús **Sistema**, **Configuración bloqueo** (funciones para el control de accesos)**, Comunicación y Configuración log**

5.1. SISTEMA

Este submenú nos permitirá configurar los siguientes 10 parámetros:

► **Nº de administradores:**

Determina el nº total de administradores registrables en el sistema. Configurable entre (1 – 10), valor por defecto: (5).

► **Idioma:**

Determina el idioma en el que se presentan los diferentes menús en el terminal.

Idioma por defecto: (Español).

► **Fecha:**

Actualización de la fecha y hora.

► **Formato fecha:**

Determina el formato de presentación de la fecha vigente (día/mes/año, año/día/mes, etc.)

► **Voz activada:**

Activa o desactiva la función de confirmación por mensajes de voz ante determinadas acciones realizadas sobre el terminal.

► **Ajuste brillo:**

Permite ajustar la luminosidad de la pantalla LCD del terminal.

► **Apagar (*):**

Permite activar el bloqueo sobre la tecla de encendido/ apagado existente en el terminal, con el fin de que éste no pueda ser apagado por cualquier persona. Por defecto esta función está desactivada.

► **Auto apagado (*):**

Permite ajustar el tiempo en minutos (1-255) para que el terminal se apague automáticamente. Por defecto esta función está desactivada.

(*)NOTA: para el correcto funcionamiento del sistema, es conveniente que ambas funciones estén desactivadas. En cualquier caso, aún estando activadas, el terminal se encenderá de forma automática a los 3 segundos aproximadamente de la desconexión (ya se realice ésta de forma manual o automática).

► **Contraste LCD:**

Permite ajustar el contraste de la pantalla de LCD del terminal.

► **Configuración inicial:**

Devuelve los paramétros de configuración a los establecidos inicialmente en fábrica.

5.2. CONTROL DE ACCESOS.

El terminal biométrico mod. MF830 cuenta con un importante paquete de funciones especialmente enfocadas al Control de Accesos. Estas funciones se explican a continuación y básicamente se centran en 2 aplicaciones:

► configuración de los **permisos** de acceso para el personal

► configuración de las **alarmas** cuando el acceso no está autorizado.

Estos son los parámetros a configurar:

► **Desbloquear:**

Configuración del tiempo de apertura de la cerradura. Por defecto: 5s. Configurable entre los valores de NO (normalmente abierto) y 255 s.

► **Apertura superada:**

Cuando el tiempo de apertura supera al configurado en el terminal, el zumbador que incorpora éste empezará a sonar. El relé de la alarma no actuará.

Desactivada la alarma por tiempo de apertura excedido, la puerta se cerrará. Valor por defecto: NO. Configurable entre 1 y 255s.

► **Apertura ilegal:**

Cuando la puerta es abierta de forma violenta y supera el tiempo de apertura establecido, el zumbador del terminal continuará sonando, y el terminal actuará dando señal (el sensor de puerta chequea que la puerta no se cierra una vez superado el tiempo establecido)

Valor por defecto: NO. Configurable entre 1 y 255s

Los siguientes 4 puntos (HORAS DE ENTRADA -GRUPO TIEMPO -DÍAS ENTRADA -DÍAS USUARIO), se refieren a la configuración de permisos para el control del acceso.

Para una más fácil comprensión es interesante tener en mente un supuesto como el que sigue:

*El trabajador Francisco Pérez tiene **acceso autorizado** a la sala de máquinas de su empresa, en los siguientes días y franjas horarias:*

► *Lunes a Jueves (de 9.30 a 14.30h y de 16.00 a 19.00h)*

► *Viernes (de 8.30 a 15.30h)*

*Se deduce por tanto que dicho trabajador tiene el **acceso denegado** los fines de semana y los días de diario en las franjas horarias no contempladas en el ejemplo anterior.*

Los parámetros que se citan a continuación pueden configurarse desde el propio terminal o desde la aplicación Access Control en sus diferentes versiones.

► **Horas de entrada (franjas horarias):**

Se pueden definir hasta 32 franjas horarias (desde la 00 a la 31), dentro del mismo día y teniendo en cuenta que:

-**La franja horaria 00** no se puede modificar desde el terminal, está definida entre las 00:00h y las 23:59h, y significa ACCESO PERMITIDO DURANTE LAS 24h.

-**La franja horaria 31** no se puede modificar desde el terminal, está definida entre las 00:00h y las 00:00h, y significa ACCESO DENEGADO DURANTE LAS 24h.

-Las restantes franjas horarias (desde la 01 a la 30) pueden ser configuradas por el usuario a su antojo, como se ejemplifica en el siguiente cuadro:

ID Franja horaria	Horario franja
01	De 6.30 a 14.30h
02	De 7.30 a 15.30h
03	De 8.30 a 16.30h
04	De 15.30 a 23.30h

La configuración por defecto del terminal es franja horaria 00, es decir, acceso permitido las 24h.

► **Grupo tiempo (grupos de franjas horarias):**

Se pueden definir hasta 32 grupos de franjas horarias (desde el 00 al 31), cada uno de los cuales engloba hasta 10 franjas horarias y teniendo en cuenta que:

-**El grupo de tiempo 00** no se puede modificar desde el terminal, y las 10 franjas horarias que engloba son todas del tipo 00, es decir, todas denotan ACCESO PERMITIDO LAS 24h.

-**El grupo de tiempo 31** no se puede modificar desde el terminal y las 10 franjas horarias que engloba son todas del tipo 31, es decir, todas denotan ACCESO DENEGADO LAS 24h.
-Los restantes grupos de tiempo (desde el 01 al 30) pueden ser configurados por el usuario a su antojo como se ejemplifica en el siguiente cuadro:

ID Grupo franjas	Grupo franjas	ID franja horaria	Horario franja
03	01	01	De 6.30 a 14.30h
	02	02	De 7.30 a 15.30h
	03	03	De 8.30 a 16.30h
	04	04	De 15.30 a 23.30h
	06	12	
	07	14	
	08	17	
	09	21	
	10	23	

El grupo de franjas horarias por defecto es el 0 para cualquier usuario registrado, es decir acceso permitido las 24h.

► **Días entrada (franjas horarias semanales):**

Se pueden definir hasta 32 grupos de franjas horarias semanales (desde el 00 al 31), cada uno de los cuales asigna grupos de franjas horarias (grupos de tiempo) a cada uno de los 7 días de la semana (de Domingo a Sábado).

-**La franja semanal 00** no se puede modificar desde el terminal. Asigna a cada uno de los 7 días de la semana el grupo de tiempo 0, el cual según hemos expuesto anteriormente, incluye un grupo de 10 franjas horarias del tipo 00.

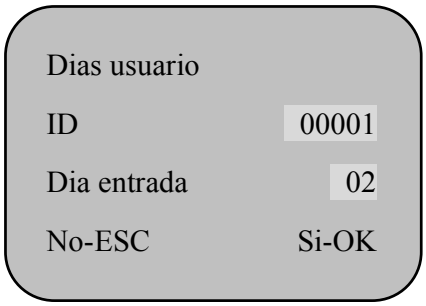
-**La franja semanal 31** no se puede modificar desde el terminal. Asigna a cada uno de los 7

días de la semana el grupo de tiempo 0, el cual según hemos expuesto anteriormente, incluye un grupo de 10 franjas horarias del tipo 00.

El grupo de franjas horarias semanal por defecto es el 0 para cualquier usuario registrado, es decir, acceso permitido las 24h , todos los días de la semana.

► **Días usuario:**

En este apartado se asigna a cada usuario registrado, la franja horaria semanal por la cual se va a regir. La configuración de este punto en el terminal se presenta como en el dibujo adjunto:



► **Tipo verificación:**

Para determinar la forma por la que el usuario va de realizar la identificación, ya sea **simple** (huellla, clave, etc.) o **combinada** (huella+clave, etc.)

► **Activación alarma:**

Para configurar la activación o no de las señales de alarma.

► **Modo alarma:**

La tercera huella registrada por un mismo usuario, es utitlizada por el terminal para la gestión de alarmas. Si la señal de alarma está activada (punto anterior) y el usuario introduce su tercera huella registrada, el sistema entiende que aquel está sufriendo una amenaza y está siendo forzado para que realice la apertura de la puerta. A partir de la introducción de la huella, se pueden configurar 3 acciones diferentes:

-Apertura de puerta: si marcamos esta opción en la configuración, al poner la huella se abrirá la puerta pero no se disparará ninguna alarma.

-Alarma: si marcamos esta opción en la configuración, al poner la huella se disparará la alarma pero no se abrirá la puerta.

-Apertura+alarma: marcando esta opción, al poner la huella se abrirá la puerta y se activará la alarma.

► **Entrada señal:**

Referido al tipo de señal de alarma. 2 señales de alarma configurables (alarma1, alarma2) , ambas con 3 opciones de configuración:

-No:

-Señal 1: se activa el relé de alarma sonora

-Señal 2: se activa el relé de alarma silenciosa

► **Fecha límite (*):**

Se puede delimitar una fecha fija a partir de la cual el usuario no tendrá permitido el acceso.

(*) esta función no está disponible en el terminal MF830

► **Formato tarjeta WG:**

El terminal MF830 permite la conexión externa de un lector de tarjetas de proximidad. Aquí se define el protocolo de transmisión Wiegand a utilizar (26 ó 34)

5.3. COMUNICACIÓN

Este submenú está referido a la configuración del tipo de comunicación que se establecerá entre el terminal y el ordenador donde está instalada la aplicación (software).

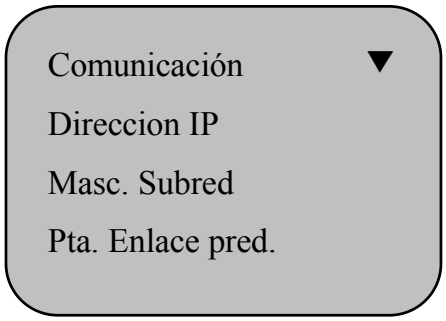
Los modos de COMUNICACIÓN

► **Comunicación vía ETHERNET/ RS485**

Es el sistema a utilizar para establecer comunicación en red.

Para establecer los parámetros de comunicación vía ETHERNET (red local), pulsamos en el

terminal la siguiente secuencia de teclas: MENU/ COMUNICACIÓN/ y marcamos la opción **Ethernet como SI,** y la opción **RS485 como NO.** Debemos ahora establecer los valores para DIRECCIÓN IP, MÁSCARA DE SUBRED y PUERTA DE ENLACE PREDETERMINADA, tal y como aparece en el dibujo de abajo.

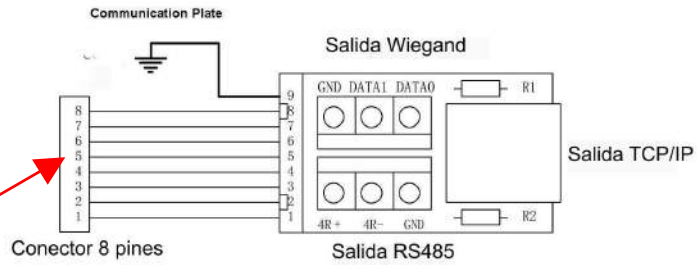


Una vez establecidos estos valores, realizaremos la conexión física del terminal al PC, router ó switch. Para ello apagamos previamente el terminal y conectamos el interface de comunicación (ver dibujo inferior) incluido con el sistema, al conector de 8 pines situado en la parte trasera del terminal. Luego conectamos a la salida TCP/IP del interface el correspondiente cable de red local.

Al encender nuevamente el terminal debe quedar establecida la comunicación.

El interface posibilita las conexiones del tipo TCP/IP, RS485 y Wiegand.

Detalle CONECTORES 8 y 16 PINES



Detalle INTERFACE COMUNICACIÓN

NOTA: la máxima distancia de comunicación utilizando cable de red local es de 1.100m. Superando esta

distancia, será necesario el uso de un repetidor.

► **ID unidad:**

Se refiere al número de terminal, teniendo en cuenta que el sistema permite el funcionamiento conjunto de hasta 255 terminales (sólo con la versión ELITE de software). El nº asignado por defecto es el (1). Si a dos o más terminales se les asignara el mismo ID, el sistema no funcionaría correctamente.

► **Baudios:**

El ratio de baudios debe ser el mismo en el ordenador y en el terminal, de lo contrarío no existiría comunicación entre ambos. El sistema permite configurar este parámetro entre los valores (9600 / 19200 / 38400). El valor por defecto es (38400). Si necesitamos cubrir distancias largas en la comunicación de los equipos, es recomendable configurar el ratio de baudios en el valor de 19.200 ya que cuanto más bajo es este valor, más estable es la comunicación y a más distancia se consigue la transmisión. Sin embargo la velocidad de transmisión se reducirá en función de la distancia.

► **Puerto nº:**

El valor del puerto seleccionado en el terminal debe coincidir con el valor del puerto del ordenador. De lo contrario no existiría comunicación entre ambos. Configurable entre los valores (1 – 9999). Valor asignado por defecto: (5005).

► **Clave:**

Definir una contraseña (hasta 6 dígitos) para el acceso a una comunicación tipo TCP/IP. El terminal sale de fábrica sin contraseña definida.

► **Dirección IP:**

Para configurar la dirección IP de la red de trabajo.

Valor por defecto: (192.168.1.224)

► **Máscara subred:**

El valor asignado por defecto es: (255.255.255.0)

► **Puerta de enlace predeterminada:**

El valor asignado por defecto es: (192.168.1.1)

► **RS485:**

El conector tipo RJ45 es válido para establecer tanto la comunicación vía RS485 como la comunicación vía ETHERNET (TCP/IP). Por tanto si pretendemos activar la comunicación vía RS485, activaremos en el menú ésta con SI y definiremos la de ETHERNET como NO.

► **Ethernet:**

El conector tipo RJ45 es válido para establecer tanto la comunicación vía ETHERNET (TCP/IP) como la comunicación vía RS485. Por tanto si pretendemos activar la comunicación vía ETHERNET, activaremos en el menú ésta con SI y definiremos la RS485 como NO.

5.4. CONFIGURACIÓN LOG

Este submenú nos permitirá configurar los siguientes 2 parámetros:

► **Aviso S-log:**

Permite configurar el disparo de un aviso cuando el número de ACTUACIONES SOBRE LA CONFIGURACIÓN DEL EQUIPO se acerque a la cantidad máxima que puede almacenar. Si no se activa esta función, el sistema no avisará cuando ya no se puedan incorporar más registros y por tanto los que superen la cantidad permitida no quedarán grabados.
Se puede ajustar entre (No – 155), de tal manera que el aviso se producirá X (la cantidad introducida) unidades antes de llegar al tope de registros. El valor por defecto es: (100).

► **Aviso G-log:**

Permite configurar el disparo de un aviso cuando el número de ENTRADAS/ SALIDAS almacenadas en el sistema se acerque a la cantidad máxima permitida por éste. Si no se activa esta función, el sistema no avisará cuando ya no se puedan incorporar más datos y por tanto éstos no quedarán grabados.
Se puede ajustar entre (No – 1.500). El valor por defecto es: (1000).

****En la aplicación de software podremos configurar el volcado automático de información con lo cual el**

terminal libera su memoria. La información volcada ya no está en el terminal pero si en la aplicación.

6. MENÚ INFORMACIÓN DEL SISTEMA

Este menú nos permitirá conocer la cantidad total almacenada de determinados valores.

► **Datos Usuario/ Administrador**

Nos aporta el nº total de USUARIOS registrados y si pulsamos OK conmutará para facilitarnos el nº total de ADMINISTRADORES registrados.

► **Datos Huella/ tarjeta / Contraseña**

Nos aporta el nº total de HUELLAS/ TARJETAS/ CONTRASEÑAS registradas. Para conmutar de un dato al otro sólo hay que pulsar la tecla OK

► **Datos LOG-G/ LOG-S**

Contabiliza el nº total de ENTRADAS/ SALIDAS realizadas y si pulsamos OK conmutará para facilitarnos el nº total de ACTUACIONES SOBRE LA CONFIGURACIÓN DEL EQUIPO.

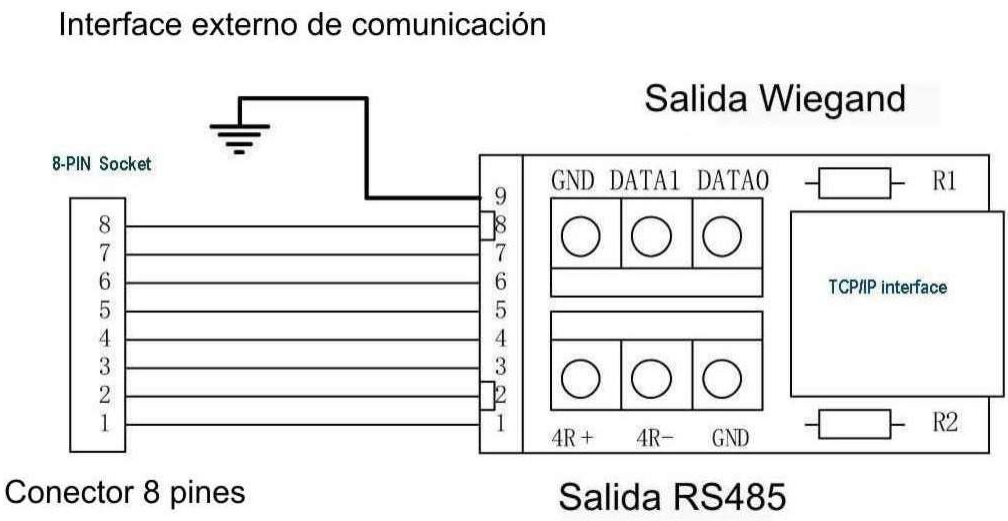
7. ESPECIFICACIONES Y ESQUEMAS TÉCNICOS

7.1. Especificaciones técnicas

Modelo	MF830
Alimentación	9-15V 120-320 mA
Relés	3A
Temperatura trabajo	0ºC / +60ºC
Niveles humedad	10%～95%
Sensor	Óptico
Placa principal	Smart KM dual-core
Algoritmo	HSA8.0
Tiempo respuesta	≤1s
Modo trabajo	Offline/online
Niveles sensibilidad	1：N y 1：1
FRR	≤1%
FAR	≤0.0001%
Modos identificación	Simple (huella, clave, tarjeta) Combinada (Huella+clave, etc.)
Total huellas	2000
Total entradas/salidas	50000
Modos comunicación	RS485、TCP/IP

Idioma	Español
Alarmas	Por apertura excedida, por apertura ilegal, por manipulación del equipo (tamper)
Bloqueo contra incendios	si
Pulsador salida	si
Weigand interface	Support WG26/WG34 in and output
Función campana	si
Función timbre	si

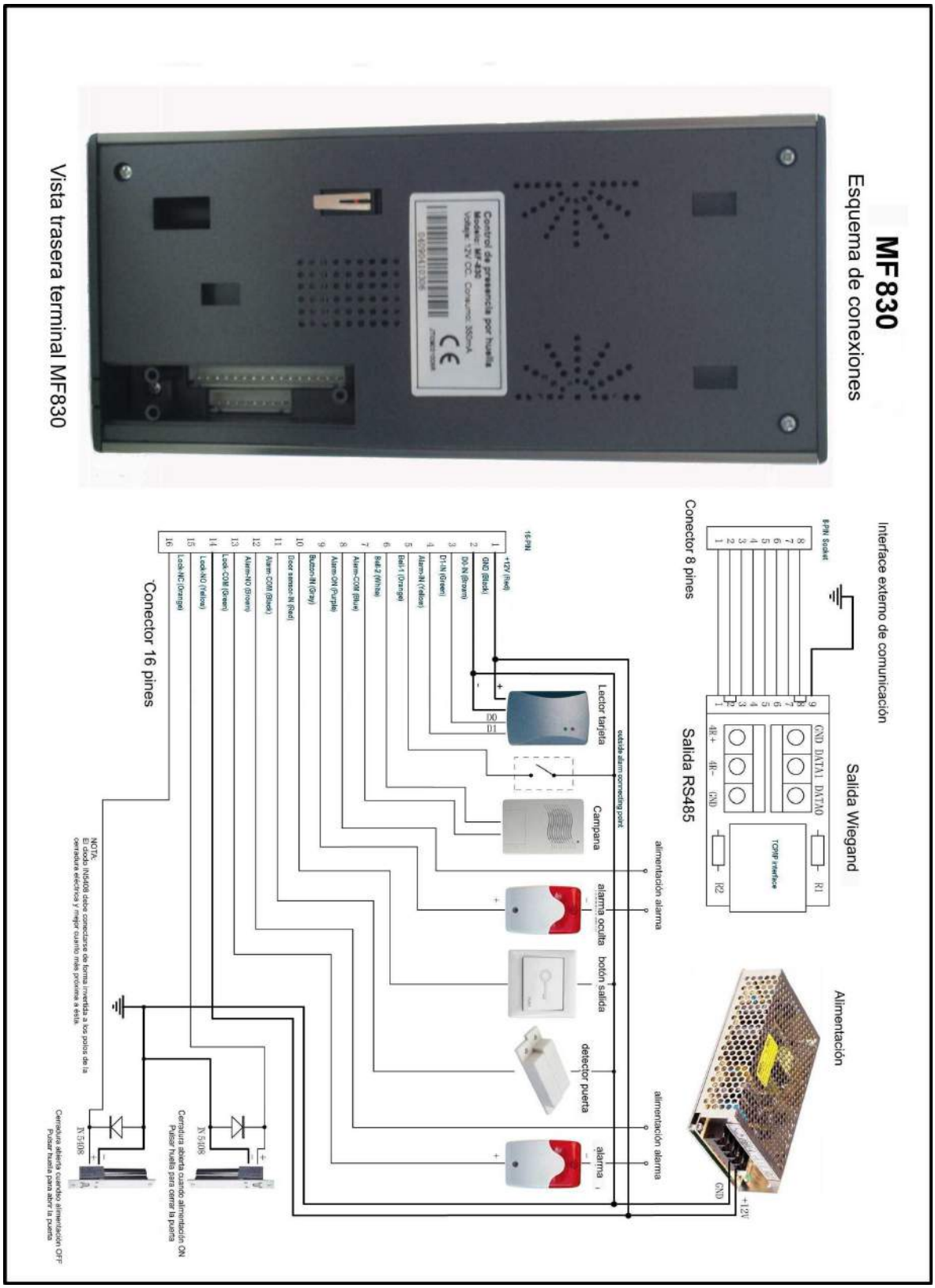
7.2. Esquemas técnicos



PIN	Definición	Descripción	Color
1	TCP_TX+	TCP/IP interface de comunicación	rojo

2	TCP_TX-		rosa
3	TCP_RX+		marrón
4	TCP_RX-		verde
5	RS485+	485+	amarillo
6	RX485-	485-	negro
7	WG_DATA0	Salida Wigand data0	blanco
8	WG_DATA1	Salida Wigand data1	azul

(1) Conector 8 pines para comunicaciones TCP/IP, RS485 y Wiegand.


MF830
Esquema de conexiones
Vista trasera terminal MF830
Interface externo de comunicación
Salida Wiegand
Salida RS485
Conector 8 pines
Conector 16 pines
Alimentación
Lector tarjeta
Campana
alarma oculta
botón salida
detector puerta
alarma
alimentación alarma
GND
DATA1
DATA0
R1
R2
+12V
GND

Pin	Definición	Descripción	Color
1	+12V IN	+12V DC (+9V — +15V)	rojo
2	GND	tierra	negro
3	D0_IN	Entrada Wigand DO	marrón
4	D1_IN	Entrada Wigand D1	verde
5	CTL_IN0	Entrada señal externa	amarillo
6	BELL_1	Entrada1 Campana	naranja
7	BELL_2	Entrada2 Campana	blanco
8	ALM1_IN	Salida señal aviso	azul
9	ALM1_OUT		purple
10	OPN_KEY	button	gris
11	OPN_SEN	Entrada sensor puerta	rojo
12	ALM0_IN	Salida señal alarma, salida señal alarma sonora	negro
13	ALM0_OUT		marrón
14	COM	Entrada alimentación cerradura	verde
15	NO	Salida apertura normal cerradura	amarillo
16	NC	Salida cerradura permance cerrada	naranja

(2) Conector 16 pines para aplicaciones en control de accesos

CE

Producto importado y distribuido por LSB, S.L. CIF: B78029527

LSB, SL C./Enero, 13 28022 Madrid e-mail: info@lsb